МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И.
Носова»

УТВЕРЖДАЮ
Директор ИГО
_____ Т.Е. Абрамзон

03.03.2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ОБРАБОТКА И ЗАЩИТА ДОКУМЕНТИРОВАННОЙ ИНФОРМАЦИИ

Направление подготовки (специальность)
46.03.02 Документоведение и архивоведение

Направленность (профиль/специализация) программы
Документоведение и документационное обеспечение управления

Уровень высшего образования - бакалавриат

Форма обучения
заочная

Институт/ факультет	Институт гуманитарного образования
Кафедра	Педагогического образования и документоведения
Курс	2

Магнитогорск
2021 год

Рабочая программа составлена на основе ФГОС ВО - бакалавриат по направлению подготовки 46.03.02 Документоведение и архивоведение (приказ Минобрнауки России от 29.10.2020 г. № 1343)

Рабочая программа рассмотрена и одобрена на заседании кафедры Педагогического образования и документоведения
08.02.2021, протокол № 7

Зав. кафедрой _____ С.С. Великанова

Рабочая программа одобрена методической комиссией ИГО
03.03.2021 г. протокол № 7

Председатель _____ Т.Е. Абрамзон

Рабочая программа составлена:
доцент кафедры ПОиД, канд. пед. наук _____ Е.П.Романов

Рецензент:

Старший менеджер (в промышленности) ПАО "ММК" ,
_____ С.А.Белобородова

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2021 – 2022 учебном году на заседании кафедры Педагогического образования и документоведения

Протокол от 14 октября 2021 г. № 4
Зав. кафедрой _____ С.С. Великанова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2022 - 2023 учебном году на заседании кафедры Педагогического образования и документоведения

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ С.С. Великанова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2023 - 2024 учебном году на заседании кафедры Педагогического образования и документоведения

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ С.С. Великанова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2024 - 2025 учебном году на заседании кафедры Педагогического образования и документоведения

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ С.С. Великанова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2025 - 2026 учебном году на заседании кафедры Педагогического образования и документоведения

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ С.С. Великанова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2026 - 2027 учебном году на заседании кафедры Педагогического образования и документоведения

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ С.С. Великанова

1 Цели освоения дисциплины (модуля)

Цель курса: сформировать у студентов теоретические знания по основам защиты информации при обращении с компьютерной техникой и программным обеспечением и, в особенности, в области применения различных сетевых технологий, а также практических навыков обеспечения защиты информации в системах обработки информации.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Обработка и защита документированной информации входит в обязательную часть учебного плана образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Математические методы в документационном обеспечении управления и архивном деле

Количественные методы в документационном обеспечении управления и архивном деле

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:

Проектная деятельность по документационному обеспечению управления организацией

Информационные технологии в документационном обеспечении управления и архивном деле

Подготовка к процедуре защиты и защита выпускной квалификационной работы

Подготовка к сдаче и сдача государственного экзамена

Практикум по составлению и оформлению служебных документов

3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «Обработка и защита документированной информации» обучающийся должен обладать следующими компетенциями:

Код индикатора	Индикатор достижения компетенции
ОПК-4 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности;;	
ОПК-4.1	Осуществляет поиск, анализ и синтез информации с использованием информационных технологий
ОПК-4.2	Применяет технологии обработки данных, выбора данных по критериям; строит типичные модели решения предметных задач по изученным образцам
ОПК-4.3	Использует современные информационные технологии для решения задач профессиональной деятельности
ОПК-5 Способен самостоятельно работать с различными источниками информации и применять основы информационно-аналитической деятельности при решении профессиональных задач.	
ОПК-5.1	Использует приемы анализа, систематизации, унификации и статистической обработки потоков информации и содержательно значимых эмпирических данных
ОПК-5.2	Выделяет и систематизирует смысловые конструкции в текстах источников, составляет и редактирует тексты служебных

	документов
ОПК-5.3	Владеет навыками рациональной информационно-поисковой работы для ведения научных исследований

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 3 зачетных единиц 108 акад. часов, в том числе:

– контактная работа – 34,6 акад. часов:

– аудиторная – 6 акад. часов;

– внеаудиторная – 28,6 акад. часов

– самостоятельная работа – 64,7 акад. часов;

– подготовка к экзамену – 8,7 акад. часа

Форма аттестации - экзамен

Раздел/ тема дисциплины	Курс	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа студента	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
1. Основные понятия теории информационной безопасности								
1.1 История становления теории информационной безопасности.	2	0,5/0,5И			4	Самостоятельное изучение учебной и научной литературы Выполнение практических и теоретических заданий	устный опрос практические работы	ОПК-4.1, ОПК-4.2
1.2 Основные термины и определения правовых понятий в области информационных отношений и защиты информации		0,5/0,5И			4	Самостоятельное изучение учебной и научной литературы Выполнение практических и теоретических заданий	устный опрос практические работы	ОПК-4.1, ОПК-4.2
1.3 Основные принципы построения систем защиты . Концепция комплексной защиты информации информации		0,5/0,5И			4	Самостоятельное изучение учебной и научной литературы Выполнение практических и теоретических заданий Выполнение задания для контрольной работы	устный опрос практические работы Задание для контрольной работы	ОПК-4.1, ОПК-4.2, ОПК-4.3, ОПК-5.3
Итого по разделу		1,5/1,5И			12			
2. Информационно-техническая безопасность								

2.1 Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности					6	Самостоятельное изучение учебной и научной литературы Выполнение практических и теоретических заданий	устный опрос практические работы	ОПК-4.1, ОПК-4.2
2.2 Построение систем защиты от угрозы нарушения конфиденциальности					6	Самостоятельное изучение учебной и научной литературы Выполнение практических и теоретических заданий	устный опрос практические работы	ОПК-4.1, ОПК-4.2, ОПК-4.3, ОПК-5.2
2.3 Угрозы информационной безопасности	2	0,5/0,5И			8	Самостоятельное изучение учебной и научной литературы Выполнение практических и теоретических заданий	устный опрос практические работы задание из контрольной работы	ОПК-4.1, ОПК-4.2, ОПК-4.3, ОПК-5.2, ОПК-5.3
2.4 Построение систем защиты от угрозы нарушения конфиденциальности				2/2И	4	Самостоятельное изучение учебной и научной литературы Выполнение практических и теоретических заданий	устный опрос практические работы	ОПК-4.1, ОПК-4.2, ОПК-4.3, ОПК-5.2
2.5 Построение систем защиты от угрозы нарушения целостности информации и отказа доступа				2/2И	8	Самостоятельное изучение учебной и научной литературы Выполнение практических и теоретических заданий	устный опрос практические работы задание из контрольной работы	ОПК-4.1, ОПК-4.2, ОПК-4.3, ОПК-5.2, ОПК-5.3
Итого по разделу		0,5/0,5И		4/4И	32			
3. Экзамен								
3.1 Подготовка к экзамену	2				20,7	Самостоятельное изучение учебной и научной литературы Выполнение индивидуального проекта по защите информации	Экзамен в устной форме Проект	ОПК-4.1, ОПК-4.2, ОПК-5.2, ОПК-5.3
Итого по разделу					20,7			
Итого за семестр		2/2И		4/4И	64,7		экзамен	
Итого по дисциплине		2/2И		4/4И	64,7		экзамен	

5 Образовательные технологии

В рамках дисциплины «Обработка и защита документированной информации» осуществляется дистанционное обучение и планируется проведение он-лайн занятий.

Дистанционное обучение - это способ получения знаний, формирования навыков и умений, основанный на интерактивном взаимодействии обучаемого с компьютером.

В ходе он-лайн-лекции предполагается трансляция презентации с обсуждением в чате текущих вопросов.

В ходе он-лайн-практика – все получают задание и готовят для обсуждения как в чате, так и в режиме вебконференции.

В учебном плане по дисциплине запланированы занятия в интерактивной форме. В связи с чем, планируется использование таких интерактивных форм работы, как работа в обсуждение дискуссионных вопросов.

Текущий, промежуточный и рубежный контроль проводится в тестовой СДО университета.

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

Представлено в приложении 1.

7 Оценочные средства для проведения промежуточной аттестации

Представлены в приложении 2.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2021. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/viewer/informacionnaya-bezopasnost-467370#page/1 - Заголовок с экрана (дата обращения: 26.04.2021).

2. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL:https://urait.ru/viewer/osnovy-informacionnoy-bezopasnosti-zaschita-informacii-475890#page/1 - Заголовок с экрана (дата обращения: 26.04.2021).

3. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В. Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2020. — 592 с. — Режим доступа:— https://znanium.com/read?id=358722 - заголовок с экрана (дата обращения: 26.04.2021).

б) Дополнительная литература:

1.Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2020. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL:
https://urait.ru/viewer/kriptograficheskie-metody-zaschity-informacii-dlya-izuchayuschih-kompyuternuyu-bezopasnost-450277#page/1 - Заголовок с экрана (дата обращения: 26.04.2021).

2. Вострецова, Е.В. Основы информационной безопасности : учебное пособие для студентов вузов / Е.В. Вострецова.— Екатеринбург : Изд-во Урал. ун-та,

2019.— 204 с — Режим доступа: http://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf - Заголовок с экрана (дата обращения: 26.04.2021).

3. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449350 (дата обращения: 26.04.2021).

в) Методические указания:

Чусавитина Г.Н., Чернова Е.В. Методические рекомендации для студентов по изучению дисциплины «Информационная безопасность»: учеб. пособие / Е.В. Чернова, Г.Н. Чусавитина. – Магнитогорск : МаГУ, 2013. – 73 с.

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
MS Windows 7 Professional(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно
7Zip	свободно распространяемое	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Информационная система - Единое окно доступа к информационным ресурсам	URL: http://window.edu.ru/
Электронные ресурсы библиотеки МГТУ им. Г.И. Носова	http://magtu.ru:8085/marcweb2/Default.asp

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Центр дистанционных образовательных технологий

Мультимедийные средства хранения, передачи и представления информации.

Комплекс тестовых заданий для проведения промежуточных и рубежных контролей.

Персональные компьютеры с пакетом MS Office, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета.

Оборудование для проведения он-лайн занятий:

Настольный спикерфон PlantronocsCalistro 620

Документ камера AverMediaAverVisionU15, Epson

Графический планшет WacomIntuosPTH

Веб-камера Logitech HD Pro C920 Lod-960-000769

Система настольная акустическая GeniusSW-S2/1 200RMS

Видеокамера купольная PraxisPP-2010L 4-9

Аудиосистема с петличным радиомикрофоном ArthurFortyU-960B

Система интерактивная SmartBoard480 (экран+проектор)

Поворотная веб-камера с потолочным подвесомLogitechBCC950 loG-960-000867

Комплект для передачи сигнала

Пульт управления презентацией LogitechWirelessPresenterR400

Стереогарнитура (микрофон с шумоподавлением)

Источник бесперебойного питания POWERCOMIMD-1500AP

Помещения для самостоятельной работы обучающихся

Персональные компьютеры с пакетом MS Office, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета

Помещение для хранения и профилактического обслуживания учебного оборудования

Шкафы для хранения учебно-методической документации, учебного оборудования и учебно-наглядных пособий.

Приложение 1

Учебно-методическое обеспечение самостоятельной работы студентов

Аудиторная самостоятельная работа студентов на данном курсе не предусмотрена.

Внеаудиторная самостоятельная работа студентов осуществляется в виде изучения лекционного курса и литературы по соответствующему разделу с проработкой материала (выполнение тестов и практических заданий).

Пример практических заданий по курсу:

1. **Информационная безопасность**

Лабораторная работа «Работа с браузером»

Ответить на следующие вопросы. Ответы продемонстрировать преподавателю в виде скриншотов или развернутого текстового описания:

1. Как установить страницу, с которой будет происходить начальная загрузка?
2. Как заблокировать рекламу, отображаемую во всплывающих окнах?
3. Как позволить отдельным ресурсам использование всплывающих окон?
4. Как составить список сайтов, доступ к которым заблокирован?
5. Как очистить кэш браузера? Для чего это нужно делать?
6. Что такое файлы «cookie», для чего они нужны, в чем их опасность?
7. Что такое «режим инкогнито» («приватный режим»)? Для чего он нужен? Как его включить?
8. Что такое «плагин»? Для чего он нужен? Как установить и удалить плагин?
9. Где хранятся пароли в вашем любимом браузере? Как получить к ним доступ?
10. Настройте синхронизацию для вашего браузера. Что это такое? Для чего необходимо использовать синхронизацию?
11. Настройте приоритетные поисковые системы в браузере.
12. Поменяйте оформление браузера по вашему вкусу.

Лабораторная работа «Настройка прав доступа

в операционной системе Windows»

Ответы продемонстрировать преподавателю в виде скриншотов или развернутого текстового описания.

Задание 1 «Создание учетной записи пользователя»

1. Создайте учетную запись для своего пользователя.
2. Тип учетной записи – с ограниченными возможностями.
3. Выберите изображение для своей учетной записи.
4. Установите пароль.
5. Установите параметр «Требовать нажатие клавиш Ctrl+Alt+Delete» («Классическое окно ввода»).
6. Отключите учетную запись «Гость» (если она есть).

Задание 2 «Установление пароля для экранной заставки»

Рабочий стол (правая кнопка мыши) ® Свойства ® Заставка

1. Выберите заставку из предложенных.
2. При необходимости настройте параметры по вашему вкусу.

3. Установите флажок «Защита паролем».
4. Проверьте. Если пароль на заставку не работает, подумайте, почему это может быть (подсказка – учетная запись пользователя).

Задание 3 «Личные папки пользователя»

Войдите в систему под своей учетной записью. Выберите папку, доступ к которой вы хотите ограничить. Щелкните на ней правой кнопкой мыши, в меню выберите Свойства ® Вкладка Доступ. Установите флажок «Отменить общий доступ к этой папке».

Лабораторная работа «Защита информации в текстовом редакторе»

Задание 1

Самостоятельно ознакомиться с возможностями настройки защиты информации в текстовом редакторе.

Задание 2

Настроить следующие способы защиты документа:

1. Документ Фамилия_Doc1 при открытии требует пароль на доступ к файлу, модификация файла запрещена (изменение текста невозможно).
2. Документ Фамилия_Doc2 открывается только для чтения.
3. Документ Фамилия_Doc3 при открытии требует пароль на доступ к файлу и редактирование (2 разных пароля).

Лабораторная работа «Защита данных с помощью архивирования»

- Создайте на рабочем диске папку «Фамилия». Скопируйте в нее файлы следующего типа *.doc, *.xls, *.jpg.

- Заархивируйте папку с паролем с помощью любой программы-архиватора. Имя архива должно быть вида «Фамилия».

- Продемонстрируйте результаты преподавателю.

2. Защита информации

Лабораторная работа «Защита личной информации при пользовании сервисами Google»

Ответы продемонстрировать преподавателю в виде скриншотов или развернутого текстового описания:

1. Просмотрите историю поисковых запросов. Отключите сохранение истории.
2. Просмотрите историю загруженных игр.
3. Просмотрите историю местоположений. Подумайте, каким образом можно отменять сохранение истории, не используя ее отключение. Попробуйте проделать эти действия. Проверьте результат в течение нескольких дней.
4. Очистите данные в настройках рекламы. Отключите сервис Google Analytics.
5. Просмотрите данные о контактах – все ли контакты вам необходимы? Настройте сведения о контактах.
6. Привяжите свой аккаунт к номеру телефона, активизируйте передачу информации о подозрительных действиях. Для чего это нужно?

7. Проверьте список устройств, с которых происходило подключение к аккаунту. Для чего это нужно? Что можно сделать с незнакомым устройством?
8. Проверьте настройки доступа к аккаунту. Просмотрите список приложений, сайтов и устройств, связанных с вашим аккаунтом Google. Убедитесь, что все они надежны, и удалите ненужные. Не забывайте очищать данный список после удаления игр и приложений. Для чего необходимо это делать?
9. Запретите непроверенным приложениям доступ к аккаунту.
10. Проверьте резервный адрес электронной почты. Для чего он необходим?
11. Что такое «двухэтапная авторизация и для чего она необходима»?
12. Настройте сохранение данных аккаунта.

Лабораторная работа «Антивирусная программа»

Задание 1

Самостоятельно познакомиться с возможностями антивирусной программы, установленной на компьютере. Изучить следующие пункты:

1. Запуск программы.

2. Основное окно программы.

3. Окно помощи.

Задание 2

Изучить особенности:

1. Проверка компьютера (полностью).

2. Запуск проверки подключаемого носителя.

- по требованию пользователя;

- автоматический запуск при подключении.

3. Контроль за контентом:

- шпионские программы;

- «заражённые» сайты;

- фишинг-атаки и пр.

Лабораторная работа «Защита информации в социальных сетях»

Рассмотрите особенности защиты информации в наиболее распространенных социальных сетях (В контакте, Одноклассники, Мой мир, Фейсбук и др.)

Ответить на следующие вопросы, доказать ответ скриншотами:

1. Доступность создания «фейковых» анкет (Ненастоящие имя, фамилия, либо использование данных известных людей)

2. Доступность закрытия информации при регистрации (дата рождения, образовательные заведения и пр.)

3. Вы обнаружили в социальной сети ваш «клон». Ваши действия? (описать со ссылками и скриншотами)

4. Вы обнаружили, что некий человек пишет вам негативные и агрессивные сообщения. Ваши действия? (показать скриншоты)

5. Имеете ли вы возможность создания определенных списков друзей, с различными уровнями допуска к вашей информации?

6. Вы разместили в своем аккаунте информацию конфиденциального характера. Каким образом вы можете ограничить доступ остальных к этой информации? (показать скриншоты) Ответить на вопрос для:

- Фотографии;
- Фотоальбома;
- Видеозаписи;
- Текстовой записи.

7. Какие действия и тексты в приложении должны заставить вас насторожиться? Что может, а чего не может просить от вас приложение?

8. Какие действия вы должны предпринять, получив подобное сообщение?

Я вообще-то с просьбой к тебе) Как-то даже неудобно спрашивать, если честно) У тебя есть рублей пятьсот мне на модем закинуть надо?) А то закончились на нем деньги. А я отдам чуть позже!)

9. Каким образом вы можете восстановить утраченный пароль?

10. Охарактеризуйте в целом возможности защиты личной информации в выбранной вами социальной сети.

Приложение 2

Оценочные средства для проведения промежуточной аттестации

а) Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации:

Код индикатора	Индикатор достижения компетенции	Оценочные средства
ОПК-4 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности;;		
ОПК-4.1	Осуществляет поиск, анализ и синтез информации с использованием информационных технологий	*Примерный перечень вопросов к экзамену в форме теста* 1. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены? a. Владельцы данных b. Пользователи c. Администраторы **d. Руководство** 2. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании? **a. Поддержка высшего руководства** b. Эффективные защитные меры и методы их внедрения c. Актуальные и адекватные политики и процедуры безопасности d. Проведение тренингов по безопасности для всех сотрудников 3. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков? a. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски b. Когда риски не могут быть приняты во внимание по политическим соображениям c. Когда необходимые защитные меры слишком сложны **d. Когда стоимость контрмер превышает ценность актива и потенциальные потери** 4. Что такое политики безопасности? a. Пошаговые инструкции по выполнению задач безопасности b. Общие руководящие требования по достижению определенного уровня безопасности **c. Широкие, высокоуровневые заявления руководства** d. Детализированные документы по обработке инцидентов безопасности 5. Какой из следующих законодательных терминов относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств? a. Стандарты b. Должный процесс (Due process) **c. Должная забота (Due care)** d. Снижение обязательств 6. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ

Код индикатора	Индикатор достижения компетенции	Оценочные средства
		безопасности? a. Список стандартов, процедур и политик для разработки программы безопасности b. Текущая версия ISO 17799 c. Структура, которая была разработана для снижения внутреннего мошенничества в компаниях **d. Открытый стандарт, определяющий цели контроля** 7. Что представляет собой стандарт ISO/IEC 27799? **a. Стандарт по защите персональных данных о здоровье** b. Новая версия BS 17799 c. Определения для новой серии ISO 27000 *Пример практического задания* Настроить следующие способы защиты документа: 4. Документ Фамилия_Doc1 при открытии требует пароль на доступ к файлу, модификация файла запрещена (изменение текста невозможно). 5. Документ Фамилия_Doc2 открывается только для чтения. 6. Документ Фамилия_Doc3 при открытии требует пароль на доступ к файлу и редактирование (2 разных пароля).
ОПК-4.2	Применяет технологии обработки данных, выбора данных по критериям; строит типичные модели решения предметных задач по изученным образцам	*Примерный перечень вопросов к обсуждению* 1. Понятие информационного общества. 2. Критерии перехода к информационному обществу. 3. Понятие информационной безопасности. 4. Основные составляющие информационной безопасности. 5. Законодательные аспекты обеспечения информационной безопасности. 6. Основные информационные проблемы обеспечения национальной безопасности. 7. Основные цели и объекты информационной безопасности страны. *Пример индивидуальных заданий*: **Задание 1. Найти ресурс Федерального Госоргана** Найдите официальный ресурс Федерального Госоргана, укажите его и поясните, почему, на ваш взгляд, он является достоверным. **Задание 2. Найти ресурс областного Госоргана** Найдите официальный ресурс областного Госоргана, укажите его и поясните, почему, на ваш взгляд, он является достоверным. **Задание 3. Найти новостной ресурс** Найдите официальный новостной ресурс, укажите его и поясните, почему, на ваш взгляд, он является достоверным. **Задание 4. Достоверность информации** Проанализируйте указанную ниже информацию и определите, является ли она истинной. Аргументируйте ответ, подкрепляя ссылками на источники. Проверьте источники на надежность и достоверность.
ОПК-4.3	Использует современные информационные	*Примерный перечень вопросов к экзамену в форме теста* 1. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из

Код индикатора	Индикатор достижения компетенции	Оценочные средства
	технологии для решения задач профессиональной деятельности	различных подразделений компании? a. Чтобы убедиться, что проводится справедливая оценка b. Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ **c. Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа** d. Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку 2. Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод: a. гаммирования; b. подстановки; c. кодирования; **d. перестановки;** 3. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод: **a. гаммирования;** b. подстановки; c. кодирования; d. аналитических преобразований. 4. Активный перехват информации - это перехват, который: a. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации; b. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций; c. неправомерно использует технологические отходы информационного процесса; **d. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.** 5. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется: a. активный перехват; b. пассивный перехват; **c. аудиоперехват;** d. видеоперехват; 6. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется: a. активный перехват; **b. пассивный перехват;**

Код индикатора	Индикатор достижения компетенции	Оценочные средства
		c. видеоперехват; d. просмотр мусора. 7. Перехват, который осуществляется путем использования оптической техники называется: a. активный перехват; b. пассивный перехват; **c. видеоперехват;** d. просмотр мусора. 8. К внутренним нарушителям информационной безопасности относится: a. клиенты; b. пользователи системы; c. сотрудники отделов разработки и сопровождения ПО; **d. технический персонал, обслуживающий здание**
ОПК-5 Способен самостоятельно работать с различными источниками информации и применять основы информационно-аналитической деятельности при решении профессиональных задач.		
ОПК-5.2	Выделяет и систематизирует смысловые конструкции в текстах источников, составляет и редактирует тексты служебных	*Пример практического задания* Подготовить доклад с мультимедиа поддержкой по одной из предложенных ниже тем 1) Оценочные стандарты и технические спецификации. Основные понятия. 2) Стандарт Министерства обороны США «Критерии оценки доверенных компьютерных систем» (Department of Defense Trusted Computer System Evaliation Criteria, TCSEC, [TCSEC]) («Оранжевая книга») как оценочный стандарт. История создания и текущий статус. Политика безопасности согласно «Оранжевой книге». Классы безопасности информационных систем по степени доверия безопасности («Оранжевая книга»). 3) Красная книга. Интерпретация критериев оценки надежности систем для сетей. Trusted Network Interpretation. 1993. (NCSC-tg-005). 4) Розовая книга. Интерпретация системы управления надежной базой данных в критериях оценки надежных компьютерных систем Министерства обороны из числа критериев оценки надежных компьютерных систем. Trasted Database Management System Interpretation of the Trusted Computer System Evaluation Criteria. NCSC, 1991, (NCSC-TG-021). 5) Информационная безопасность распределенных систем. Рекомендации X.800 «Архитектура безопасности для взаимодействия открытых систем» . 6) Спецификация Internet-сообщества RFC 1510 «Сетевой сервис аутентификации Kerberos (V5)» [Kerb].
ОПК-5.3	Владеет навыками рациональной информационно-поисковой работы для ведения научных исследований	*Пример комплексного задания*: – Выбрать тему исследовательского проекта, подобрать научные источники – Подобрать информационные ресурсы и сервисы для своего исследовательского проекта – Разработать план работы над исследовательским проектом – В соответствии с изученными алгоритмами разработать научный аппарат исследования

Код индикатора	Индикатор достижения компетенции	Оценочные средства
		– В соответствии с изученными алгоритмами оценить результаты исследовательского проекта

б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания:

Промежуточная аттестация проводится в форме экзамена.

При подготовке к экзамену особое внимание следует обратить на следующие моменты:

1. Регулярное прочтение (не меньше трёх раз) и осмысление теоретического материала;

2. Выполнение практических заданий с опорой на теоретический комментарий и образцы;

3. Постоянную и добросовестную работу на практических занятиях, а также самостоятельную работу.

Критерии оценки (в соответствии с формируемыми компетенциями и планируемыми результатами обучения):

- на оценку **«отлично»** – студент должен показать высокий уровень знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам, оценки и вынесения критических суждений;
- на оценку **«хорошо»** – студент должен показать знания не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам;
- на оценку **«удовлетворительно»** – студент должен показать знания на уровне воспроизведения и объяснения информации, интеллектуальные навыки решения простых задач;
- на оценку **«неудовлетворительно»** – студент не может показать знания на уровне воспроизведения и объяснения информации, не может показать интеллектуальные навыки решения простых задач.